IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Robert Bruce Hirsh
Serial No. : 09/894,919
Filed : June 29, 2001
Title : LEVERAGING A PERSISTENT CONNECTION TO ACCESS A SECURED SERVICE

Art Unit : 2131
Examiner : Cervetti, David Garcia

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

(1) Real Party in Interest

America Online, Inc., the assignee of this application, is the real party in interest.

(2) Related Appeals and Interferences

There are no related appeals or interference.

(3) Status of Claims

Claims 67-80 are pending, with claim 67 being independent. Appellant is submitting concurrent with this brief an amendment canceling claims 20, 21, 24-28, 30-39, 55-66 and 81-95. All of the pending claims stand rejected. Appellant appeals the rejections of claims 67-80.

(4) Status of Amendments

On August 2, 2005, an after-final response was filed. The August 2, 2005 response did not amend any of the pending claims and was entered as indicated by an Advisory Action on August 17, 2005. On August 25, 2005, a second after-final response was filed. The August 25, 2005 response also did not include an amendment to the claims, yet it was denied entry, as indicated by a September 16, 2005 Advisory Action. A Notice of Appeal was filed on October 3, 2005.

To simplify issues for appeal, appellant is submitting concurrent with this appeal brief an amendment canceling claims 20, 21, 24-28, 30-39, 55-66 and 81-95. Appellant respectfully

requests entry of this amendment. For convenience, the appendices of this appeal brief include both the claims after entry of this amendment and the claims prior to entry of this amendment.

(5) Summary of Claimed Subject Matter

The currently appealed claims are directed to providing access to a secured service. The following summarizes independent claim 67, which is the single independent claim involved in this appeal, and salient dependent claims 73, 79 and 80.

Independent claim 67 is directed to a method performed by a client, such as, for example, client 110, of leveraging a connection with an intermediary, such as, for example, a persistent connection service 130 and a broker service 140, to access a secured service, such as, for example, a secured service 170. See, for example, Figs. 1-3 in the application specification. In one particular example, a user request for access to the secured service 170 is received by the client system 110. See, for example, operations 410 and 505 described in the application specification on pages 7 and 10 and illustrated in Figs. 4 and 5. The client system submits a request, which is based on the user request, for access to the secured service to an intermediary that is physically distinct from the secured service. See, for example, operations 410, 510, and 515 described in the application specification on pages 7 and 10 and illustrated in Figs. 4 and 5. The client system receives from the intermediary constrained authorization information that has been authenticated by the secured service responsive to the client request. See, for example, operations 430, 431, 433, 435 and 705-735 described in the application specification on pages 8-11 and illustrated in Figs. 4 and 7. The client submits the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary. See, for example, operations 450, 451, 453, 455 and 805-820 described in the application specification on pages 8-11 and in Figs. 4 and 8.

Dependent claim 73, which depends from claim 67, is directed to a method of leveraging a connection with an intermediary to access a secured service, as described above, but additionally specifies that the constrained authorization information includes one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined

time, and a constraint that the authorization information be received only from the client. See, for example, the application specification at pages 9, 10 and 12 and Fig. 8.

Dependent claim 79, which depends from claim 67, is directed to a method of leveraging a connection with an intermediary to access a secured service, as described above, but additionally specifies that the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary. See, for example, the application specification at pages 1, 5, and 8.

Dependent claim 80, which depends from claim 67, is directed to a method of leveraging a connection with an intermediary to access a secured service, as described above, but additionally specifies that the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary. See, for example, the application specification at pages 1, 5, and 8.

(6) Grounds of Rejection

Independent claim 67 and its dependent claims 68-80 have been rejected under 35 U.S.C. §103(a) as being obvious over Cohen (U.S. Patent No. 6,178,511)

(7) Issues

(a) The subject matter of independent claim 67 and its dependent claims 68-72 and 74-78 is not obvious in view of the teachings of Cohen because Cohen fails to teach or suggest "receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request" and "submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary."

(b) The subject matter of dependent claims 73, 79 and 80 is not obvious in view of the teachings of Cohen and the references additionally mentioned in the Advisory Action of

August 17, 2005 (hereinafter referred to as the "Added References")[1] because neither Cohen, the Added References, nor any proper combination thereof teaches or suggests the above-noted features.

(c) The Added References have not been properly cited by the Examiner to support the rejections.

(8) Grouping of Claims

The claims do not stand or fall together. Rather, as apparent from the above-stated issues, the claims involved in this appeal, claims 67-80, may be considered in two groups.

(1) Claims 67-72 and 74-78 which recite, among other distinguishing features and feature combinations, "receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request" and "submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary."

(2) Claims 73, 79 and 80, which depend from claim 67, and thus incorporate the above-noted distinguishing features, and which also recite features that were recognized by the Examiner as falling outside of the scope of Cohen, and which therefore necessitated an improper combination by the Examiner of Cohen with the Added References.

(9) Argument

Appellants submit the following arguments in support of reversal of the rejections of the above-listed claims as being obvious over Cohen.

(a) The subject matter of independent claim 67 and its dependent claims 68-72 and 74-78 is not obvious in view of the teachings of Cohen

Independent claim 67 relates to a "method, performed by a client, of leveraging a connection with an intermediary to access a secured service" and recites, among other things,

---

[1] Specifically, the Added References include: the Handbook of Applied Cryptography by Menezes et al, Chapter 10, pages 385-424; Hardy et al. (U.S. Patent No. 6,073,242); and Thompson et al. (U.S. Patent No. 6,668,253).

"receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request" and "submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary." Cohen fails to describe or suggest at least these features of claim 67.

Cohen describes a single sign-on (SSO) system in which a user signs on to the SSO system one time and the SSO system signs the user on to other applications. (Cohen at col. 2, lines 29-32). For each user, the SSO system securely stores that user's username, password, and other pertinent login information for each other application that the user may wish to access. (Id. at col. 4, line 61 to col. 5, line 6). This information has been previously entered into the SSO system by the user. (Id. at col. 5, lines 45-57). Once the user has logged in to the SSO system, the SSO system accesses that user's stored usernames, passwords, and other login information for the other applications, and automatically logs the user in to the other applications. (Id. at col. 6, lines 8-45). The SSO system of Cohen thus provides a method of leveraging stored user information to enable user login to multiple applications. (Id. at col. 6, lines 46-48).

Notably, in Cohen, the user does not receive constrained authorization information from the SSO system (which the Final Office Action equates to the claimed intermediary) that has been authenticated by the application (which the Final Office Action equates to the claimed secured service). The user also does not submit the constrained authorization information to the application to establish a direct connection with the application independent of the connection between the user and the SSO service. Rather, in Cohen, the SSO system directly authenticates the user to the application by using the user's own stored username and password, and the user accesses the application through the connection that the user has established with the SSO service.

The Final Office Action acknowledges that Cohen fails to describe or suggest "submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary." However, the Final Office Action fails to recognize that Cohen actually teaches an alternative to such a

process – showing submissions of credentials by the SSO rather than the claimed submission by the client. Moreover, failing to recognize the extent of the alternative teaching of Cohen, the Final Office Action takes Official Notice "that the use of client-server communications independent of an intermediary was conventional and well known."

This use of Official Notice, however, has three problems: (1) the Official Notice fails to meet the recited limitations for which Cohen is deficient and for which the Official Notice is relied upon; (2) the features that were noticed are not believed to have been conventional and well known at the time of the invention, at least in the context of claim 67; and (3) the Final Office Action's suggestion that Cohen is properly combined with teachings required to meet the claimed limitations, whether present in the art referenced by the Official Notice or some other referenced material, assumes that it is proper to modify Cohen in this fashion – an assumption that is not accurate since it requires an improper picking and choosing of the relied upon Cohen features to the exclusion of other Cohen features that suggest an alternative to the teachings being combined with Cohen.

With respect to problem (1), even accepting for the sake of argument that the Examiner's use of Official Notice is proper, the rejection of claim 67 is improper because the facts for which Official Notice is taken do not remedy the deficiencies of Cohen. The "use of client-server communications independent of an intermediary" does not meet the claim feature of "submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary." That is, even if clients and servers were known to communicate without an intermediary, this does not mean that it would have been obvious to modify Cohen so that the user receives constrained authorization information from the SSO system and submits that information to the other application to enable communications between the client and the other application independent of the SSO system.

Indeed, Cohen teaches away from the proposed modification. Cohen teaches that the user accesses the application transparently through the SSO service by allowing the SSO service to automatically log the user into the application using the user's own username and password. In contrast, claim 67 recites that the client receives constrained authentication information from the intermediary and submits that information to establish a connection with the secured service

independent of the intermediary. Only through the impermissible use of hindsight would it have been obvious to modify Cohen in the way proposed in the Office Action.

With respect to problem (2), neither the Final Office Action nor the subsequent two advisory actions provide documentary support that "that the use of client-server communications independent of an intermediary was conventional and well known." The Examiner's explanation in the advisory action of August 17, 2005 that "client-server communications were also conventional and well known, thus the name client-server architecture, because client stations accessed a server via a network without the use of an intermediary" is not sufficient documentary evidence to support the taking of the Official Notice.

With respect to problem (3), the Final Office Action's combination of Cohen with Officially Noticed teachings is an improper picking and choosing of features of Cohen to the exclusion of other Cohen features that suggest an alternative to the Officially Noticed teachings combined with Cohen. Such a picking and choosing is based on an impermissible use of hindsight and is improper. *SmithKline Diagnostics, Inc. v. Helena Laboratories Corp.*, 859 F.2d 878, 8 USPQ2d 1468 (Fed. Cir. 1988) (A challenger to the validity of a patent "cannot pick and choose among the individual elements of assorted prior art references to recreate the claimed invention."). Specifically, the Final Office Action relies upon the teachings of Cohen as disclosing all of the claim 67 features except for the claimed submission of authorization information by the client. The Final Office Action then conveniently neglects the teachings of Cohen, which show submission of credentials by the SSO system rather than by the client, and relies upon Officially Noticed teachings as disclosing the remaining claimed submission of authorization information by the client.

For at least the foregoing reasons, appellant respectfully requests reversal of the rejections of claim 67, and its dependent claims 68-72 and 74-78.

(b) The subject matter of dependent claims 73, 79 and 80 is not obvious in view of the teachings of Cohen and the Added References

In the advisory action of August 17, 2005, the Examiner cited the Added References in support of the Official Notice taken in the Final Office Action that the following features related to dependent claims 73, 79 and 80 are conventional and well known: "the use of a threshold

number, a time window, and to receive the information from the client attempting access to information, to limit use of authorization information" (claims 73); and "the use of direct authentication by a user" (claims 79 and 80). Even assuming for the sake of argument that these references properly support the Examiner's Official Notice position, appellant respectfully submits that the Added References do not describe or suggest, nor have they been relied upon as disclosing, the above-noted distinguishing features of claim 67 incorporated into claims 73, 79 and 80 through their dependency. Moreover, to the extent these features were conventional and well known, the Examiner has provided no motivation or suggestion for making the proposed modifications to Cohen based on these features.

For at least these additional reasons, appellant respectfully requests the reversal of the rejections of claims 73, 79, and 80.

(c) The Rejections Based on the Added References Are Improper

Appellant respectfully submits that the Added References have not been cited in a PTO-892 and, therefore, may not be properly used as cited art in support of claim rejections. Because of their submission as part of an advisory action, appellant is neither receiving the time nor the credit for establishing the patentability of the pending claims over the newly Added References.

For at least the above reasons, appellant respectfully requests that the rejections of claims 67-80 be reversed.

Please apply the amount of $450.00 for the Petition for Extension of Time fee and the amount of $500 for the Appeal Brief to Deposit Account Number 06-1050.

Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 2/3/06

Roberto J. Devoto
Reg. No. 55,108

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

Appendix of Claims I – After Entry of Amendment Submitted Concurrently with Appeal Brief

1-66. (cancelled).

67. (previously presented) A method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method comprising:

receiving a user request for access to a secured service;

submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service;

receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request; and

submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary.

68. (previously presented) The method of claim 67 wherein establishing the authenticated connection between the client and the intermediary comprises:

sending, by the client, keystone authentication information to the intermediary; and

receiving, from the intermediary, verification of the keystone authentication information.

69. (previously presented) The method of claim 68 wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information.

70. (previously presented) The method of claim 69 wherein the intermediary is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication.

71. (previously presented) The method of claim 67 wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary.

72. (previously presented) The method of claim 67 wherein the constrained information has been provided by the intermediary and authenticated by the secured service.

73. (previously presented) The method of claim 67 wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

74. (previously presented) The method of claim 67 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

75. (previously presented) The method of claim 67 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

76. (previously presented) The method of claim 67 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

77. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises an explicit request for access by the client.

78. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service.

79. (previously presented) The method of claim 67 wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary.

80. (previously presented) The method of claim 67 wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary.

81-95. (Canceled)

Appendix of Claims II – Prior to Entry of Amendment Submitted Concurrently with Appeal Brief

1-19. (cancelled).

20. (previously presented) A method, performed by an intermediary, of leveraging a persistent connection with a client to provide the client with access to a secured service, the method comprising:

receiving a first request from a client at an intermediary, the first request relating to a request for access to the intermediary;

establishing a persistent connection between the client and the intermediary in response to the first request from the client;

receiving a second request from the client at the intermediary, the second request relating to a request for access to a secured service;

authenticating the intermediary to the secured service responsive to the second request; and

enabling access by the client to the secured service conditioned on whether the intermediary is successfully authenticated to the secured service.

21. (previously presented) The method of claim 20 wherein:

establishing the persistent connection with the client includes authenticating the client to the intermediary based on keystone authentication information provided by the client; and

authenticating the intermediary to the secured service is performed without provision by the client of authentication information duplicative or additional to the keystone information used to establish the persistent connection.

22-23. (cancelled).

24. (previously presented) The method of claim 20 wherein the intermediary is authenticated to the secured service before the client is enabled access to the secured service.

25. (original) The method of claim 20 wherein establishing the persistent connection comprises:

receiving keystone authentication information from the client;

authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection; and

establishing the persistent connection with the client based on the keystone authentication.

26. (previously presented) The method of claim 25 wherein the second request from the client for connection to the secured service is received after the persistent connection to the client is established.

27. (previously presented) The method of claim 26 wherein authenticating the intermediary to the secured service includes:

providing a leveraged authentication based on the keystone authentication associated with the persistent connection; and

using the leveraged authentication to establish a connection with the secured service.

28. (original) The method of claim 27 wherein the keystone authentication is used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

29. (cancelled).

30. (previously presented) The method of claim 20 wherein the intermediary comprises a persistent connection service that establishes the persistent connection with the client and a broker service that authenticates the intermediary to the secured service, and authenticating the intermediary includes the broker service receiving from the persistent connection service at a

connection request address a communication based on the second request from the client and wherein the connection request address varies systematically with time.

31. (previously presented) The method of claim 20 wherein authenticating the intermediary to the secured service comprises:

determining authorization information based on the second request from the client;

communicating, to the secured service, an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information;

receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and

enabling the client to present the authorization information to the secured service to establish the connection with the secured service.

32. (previously presented) The method of claim 20 wherein authenticating the intermediary to the secured service comprises:

communicating, to the secured service, an indication that the client desires to connect to the secured service;

receiving a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes authorization information; and

communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

33. (original) The method of claim 32 wherein the authorization information is determined by the secured service.

34. (previously presented) The method of claim 20 wherein:

authenticating the intermediary to the secured service comprises communicating with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

the authorization information comprises constraint information; and

the authorization information may be ineffective to establish a connection with the secured service if one or more connection constraints indicated by the constraint information are not satisfied.

35. (original) The method of claim 34 wherein the connection constraints include a constraint that limits a number of uses for the authorization information to a predetermined threshold number.

36. (original) The method of claim 34 wherein the connection constraints include a constraint that the number of times that the authorization information has been used not exceed a predetermined number of times.

37. (original) The method of claim 34 wherein the connection constraints include a one-time-use password.

38. (original) The method of claim 34 wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window.

39. (original) The method of claim 34 wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered.

40-54. (cancelled).

55. (previously presented) The method of claim 20 wherein enabling access by the client to the secured service comprises enabling the client to access the secured service independent of the intermediary.

56. (previously presented) The method of claim 55 wherein enabling the client to access the secured service comprises enabling the client to leverage a connection other than the persistent connection established between the client and the intermediary.

57. (previously presented) The method of claim 55 wherein enabling the client to access the secured service comprises providing constrained authentication information to the client.

58. (previously presented) The method of claim 57 wherein the constrained authentication information is provided to the intermediary by the secured service.

59. (previously presented) The method of claim 58 wherein the constrained authentication information is determined by the intermediary and authenticated by the secured service.

60. (previously presented) The method of claim 20 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

61. (previously presented) The method of claim 20 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

62. (previously presented) The method of claim 20 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

63. (previously presented) The method of claim 20 wherein the intermediary is authenticated to the secured service as a consequence of the second request.

64. (previously presented) The method of claim 20 wherein the request for access to the secured service comprises an explicit request for access by the client.

65. (previously presented) The method of claim 20 wherein the request for access to the secured service comprises a client communication received via the secured service.

66. (previously presented) The method of claim 20 wherein the secured service is available for direct authentication by a user without establishing a persistent connection between the user and the intermediary.

67. (previously presented) A method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method comprising:

receiving a user request for access to a secured service;

submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service;

receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request; and

submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary.

68. (previously presented) The method of claim 67 wherein establishing the authenticated connection between the client and the intermediary comprises:

sending, by the client, keystone authentication information to the intermediary; and

receiving, from the intermediary, verification of the keystone authentication information.

69. (previously presented) The method of claim 68 wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information.

70. (previously presented) The method of claim 69 wherein the intermediary is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication.

71. (previously presented) The method of claim 67 wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary.

72. (previously presented) The method of claim 67 wherein the constrained information has been provided by the intermediary and authenticated by the secured service.

73. (previously presented) The method of claim 67 wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

74. (previously presented) The method of claim 67 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

75. (previously presented) The method of claim 67 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

76. (previously presented) The method of claim 67 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

77. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises an explicit request for access by the client.

78. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service.

79. (previously presented) The method of claim 67 wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary.

80. (previously presented) The method of claim 67 wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary.

81. (previously presented) A method, performed by a secured service, of allowing a client access based on an authenticated connection between the client and an intermediary, the method comprising:

receiving, at a secured service and from an intermediary, notification of a request by a client to access the secured service;

determining whether a trusted relationship exists between the secured service and the intermediary, responsive to the client request; and

conditioned on the existence of a trusted relationship between the secured service and the intermediary, enabling access by the client to the secured service.

82. (previously presented) The method of claim 81 wherein enabling access by the client comprises issuing constrained authorization information to the intermediary for use by the client to access the secured service.

83. (previously presented) The method of claim 82 wherein enabling access by the client further comprises receiving the constrained authorization information from the client.

84. (previously presented) The method of claim 82 wherein the constrained authorization information comprises one or more of a constraint that the authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

85. (previously presented) The method of claim 81 wherein enabling access by the client comprises authenticating constrained authorization information to be provided by the intermediary to the client to access the secured service.

86. (previously presented) The method of claim 85 wherein enabling access by the client further comprises receiving the constrained authorization information from the client.

87. (previously presented) The method of claim 85 wherein the constrained authorization information comprises one or more of a constraint that the authorization information be used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

88. (previously presented) The method of claim 81 wherein enabling access by the client comprises establishing a connection with the client independent of the intermediary.

89. (previously presented) The method of claim 88 wherein the connection between the client and the secured service is established by the client leveraging a connection other than a connection between the client and the intermediary.

90. (previously presented) The method of claim 81 wherein determining whether a trusted relationship exists between the secured service and the intermediary comprises receiving authentication information from the intermediary.

91. (previously presented) The method of claim 90 wherein the intermediary provides the authentication information to the secured service without provision by the client of other authentication information that is duplicative or additional to keystone authentication information provided by the client to the intermediary to establish the authenticated connection between the client and the intermediary.

92. (previously presented) The method of claim 81 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

93. (previously presented) The method of claim 81 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

94. (previously presented) The method of claim 81 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

95. (previously presented) The method of claim 81 wherein the secured service is available for direct authentication by a user without determining whether a trusted relationship exists between the secured service and the intermediary.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Robert Bruce Hirsh	Art Unit	: 2131
Serial No.	: 09/894,919	Examiner	: Cervetti, David Garcia
Filed	: June 29, 2001		
Title	: LEVERAGING A PERSISTENT CONNECTION TO ACCESS A SECURED SERVICE		

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT SUBMITTED CONCURRENTLY WITH APPEAL BRIEF ON FEBRUARY 3, 2006

Please amend the above-identified application as follows:

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-66. (cancelled).

67. (previously presented) A method, performed by a client, of leveraging a connection with an intermediary to access a secured service, the method comprising:

receiving a user request for access to a secured service;

submitting, by the client, a request, which is based on the user request for access to a secured service, to an intermediary that is physically distinct of the secured service;

receiving, from the intermediary, constrained authorization information that has been authenticated by the secured service, responsive to the client request; and

submitting, by the client, the constrained authorization information to the secured service to establish a direct authenticated connection between the client and the secured service independent of the authenticated connection between the client and the intermediary.

68. (previously presented) The method of claim 67 wherein establishing the authenticated connection between the client and the intermediary comprises:

sending, by the client, keystone authentication information to the intermediary; and

receiving, from the intermediary, verification of the keystone authentication information.

69. (previously presented) The method of claim 68 wherein submitting the request to the intermediary for access to the secured service prompts the intermediary to authenticate itself to the secured service without provision by the client of authentication information duplicative or additional to the keystone information.

70. (previously presented) The method of claim 69 wherein the intermediary is authenticated to the secured service by provision, by the intermediary, of a leveraged authentication based on the keystone authentication.

71. (previously presented) The method of claim 67 wherein the constrained authorization information has been issued by the secured service and sent by the secured service to the intermediary.

72. (previously presented) The method of claim 67 wherein the constrained information has been provided by the intermediary and authenticated by the secured service.

73. (previously presented) The method of claim 67 wherein the constrained authorization information comprises one or more of a constraint that the authorization information has been used no more than a predetermined number of times, a constraint that the authorization information be used within a predetermined time, and a constraint that the authorization information be received from only the client.

74. (previously presented) The method of claim 67 wherein the client comprises one or more of a web browser, an e-mail client, a synchronization client, an instant messaging client, a software productivity application, an operating system, and an operating system kernel.

75. (previously presented) The method of claim 67 wherein the intermediary comprises one or more of an instant messaging service, an e-mail service, a login service, an authentication service, an authorization service, a persistent connection service, and a broker service.

76. (previously presented) The method of claim 67 wherein the secured service comprises one or more of an e-mail service, a synchronization service, a print service, a file access service, an instant messaging service, an operating system, an operating system kernel, an authentication service, an authorization service, and a persistent connection service.

77. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises an explicit request for access by the client.

78. (previously presented) The method of claim 67 wherein the client request for access to the secured service comprises a communication sent by the client to the intermediary via the secured service.

79. (previously presented) The method of claim 67 wherein the secured service is available for direct authentication by a user without the user establishing an authenticated connection between the user and the intermediary.

80. (previously presented) The method of claim 67 wherein the direct authenticated connection between the client and the secured service is established by leveraging a connection other than the authenticated connection between the client and the intermediary.

81-95. (Canceled)

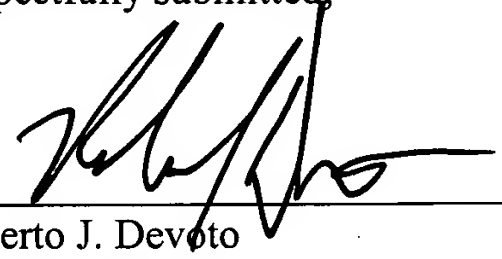
REMARKS

Claims 67-80 are pending, with claim 67 being independent. Claims 20, 21, 24-28, 30-39, 55-66 and 81-95 have been canceled to simplify issues for appeal. Applicants respectfully request that this amendment, submitted concurrently with an appeal brief, be entered.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/3/06



Roberto J. Devoto
Reg. No. 55,108

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331